PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-132457
(43)Date of publication of application : 10.05.2002

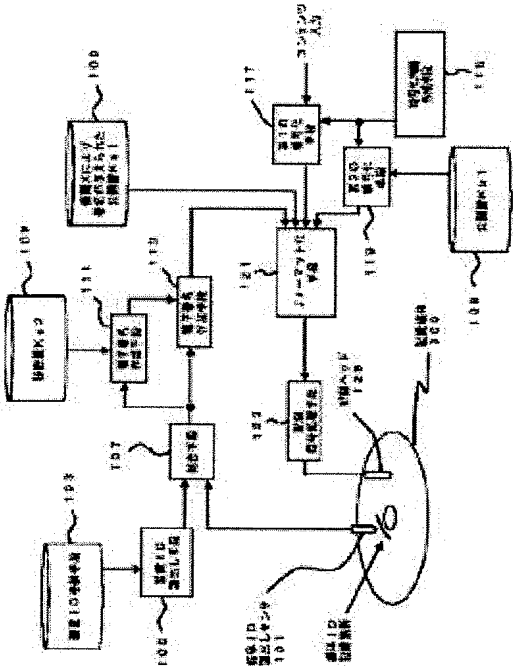
(51)Int.Cl. G06F 3/06
G06F 12/14
G09C 1/00
G11B 20/10
H04N 5/91

(21)Application number : 2000-327591
(22)Date of filing : 26.10.2000

(71)Applicant : VICTOR CO OF JAPAN LTD
(72)Inventor : OISHI TAKESHI

(54) INFORMATION RECORDING DEVICE, INFORMATION REPRODUCING DEVICE AND INFORMATION RECORDING/REPRODUCING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To make it impossible to make a copy from a recording medium and to produce plural copied recording media even if a device ID of an information recording device with which contents have been recorded is stolen or illegally altered.
SOLUTION: To combined ID data, being stored in the device ID storing means 103 of the information recording device, which is a combination of the device ID that permits the information recording device to be identified or a group ID to which the information recording device belongs and a medium ID that permits the recording medium 300 to be identified, an electronic signature adding means 113 adds an electronic signature to generate data, which are stored in the recording medium together with the contents. Thereby, only if it is confirmed that the information reproducing device is the device identical with the information recording device with which the contents have been recorded or is the device belonging to the group which is set so that it can reproduce the contents, and that the contents are recorded on the recording medium identical with the recording medium on which the information recording device has recorded the contents, the contents can be reproduced.



Japanese Unexamined Patent Application Publication No. 2002-132457

SPECIFICATION <EXCERPT>

[0039] Next, the determination of whether to permit a reproduction of content in Step S36 is described in detail. FIG. 7 is a flowchart showing an example of the operation for the determination of whether to permit a reproduction of content in Step S36 shown in the flowchart of FIG. 6. The operation regarding whether to permit a reproduction is performed in such a manner that a microcomputer in the information reproducing apparatus reads required data as appropriate into a memory in the microcomputer in the information reproducing apparatus. After Step S35, a flag P indicating whether to permit a reproduction is initialized and set to be P = 0. Here, the flag P indicating whether to permit a reproduction shows prohibiting a reproduction when P = 0, and shows permitting a reproduction when P = 1. Moreover, when the determination of whether to permit a reproduction is not completed, a reproduction is prohibited (P = 0).

[0040] Next, in Step S42, whether or not an electronically signed public key Ks1 is authorized is determined using a public key Kx1 that the reproducing device has received from an organization X. Since the electronic signature that protects the public key Ks1 is created from a secret key Kx2 which cannot be known by people outside the organization X, it is impossible for a third party to create a correct electronic signature. Accordingly, even if the third party replaces a pair of the public key Ks1 and the secret key Ks2 with another pair without authorization, it is determined to be incorrect in this verification. When the public key Ks1 is determined to be incorrect in Step S42, the determination ends in Step S99 while the flag indicating whether to permit a reproduction remains P = 0, and decryption of the content is prohibited. In addition, in the case where the electronic signature is applied to concatenated data of the public key Ks1 and an

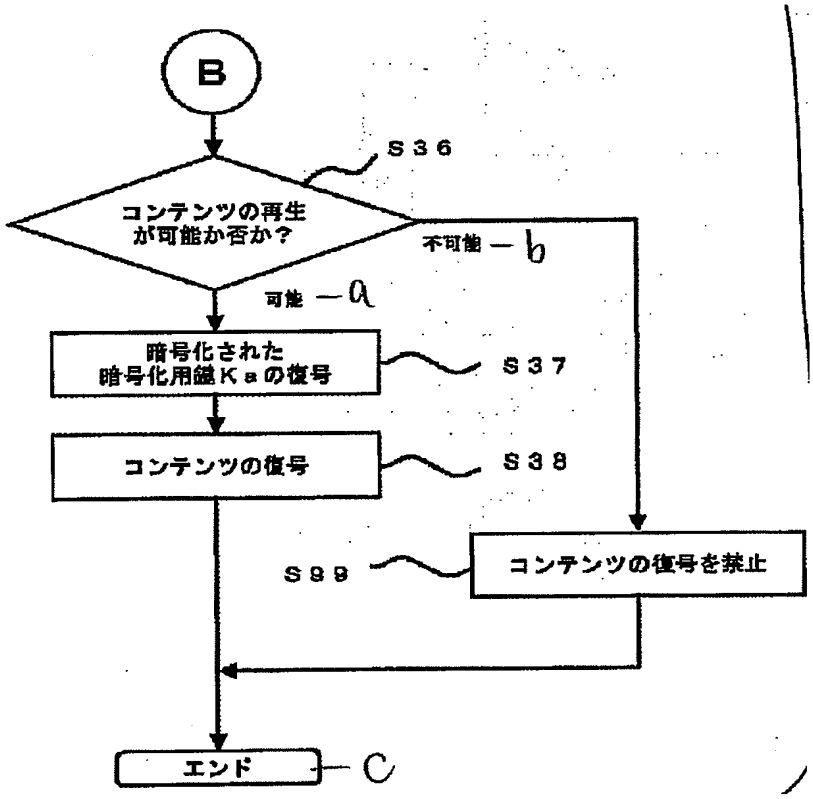
apparatus ID, it can be verified whether or not the public key Ks1 is reliably the public key for the apparatus in addition to whether or not the public key Ks1 itself is tampered, by verifying whether or not the concatenated data has correctly been transmitted.

[0041] When the public key Ks1 is determined to be correct in the verification in Step S42, in Step S43, it is determined whether or not the electronically signed concatenated ID data is authorized using the public key Ks1 determined to be authorized in Step S42. Even if the third party tampers the apparatus ID and a medium ID stored in a recording medium 300, it is determined to be incorrect in this verification. When the concatenated ID data is determined to be incorrect in Step S43, the determination ends in Step S99 while the flag indicating whether to permit a reproduction remains P = 0, and decryption of the content is prohibited.

[0042] When the concatenated ID data is determined to be correct in the verification in Step S43, in Step S44, the concatenated ID data is separated into the apparatus ID and the medium ID. Next, in Step S45, it is determined whether or not the apparatus ID of the information reproducing apparatus read out in Step S31 and the medium ID of the recording medium 300 read out in Step S32 are the same as the apparatus ID and the medium ID separated from the concatenated ID data in Step S44, respectively. When it is determined that the apparatus IDs and the medium IDs are both the same in Step S45, in Step S46, the flag P indicating whether to permit a reproduction is set to be P = 1. On the other hand, when both of the IDs or either pair is not the same , the determination ends in Step S99 while the flag indicating whether to permit a reproduction remains P = 0, and decryption of the content is prohibited. In addition, the flag P indicating whether to permit a reproduction is set as follows: when P = 1, a reproduction is permitted, and when P = 0, a reproduction is prohibited.

DRAWINGS

FIG. 6



S36: Reproduction of content is permitted?

S37: Decrypt encrypted key Ka for encryption

S38: Decode content

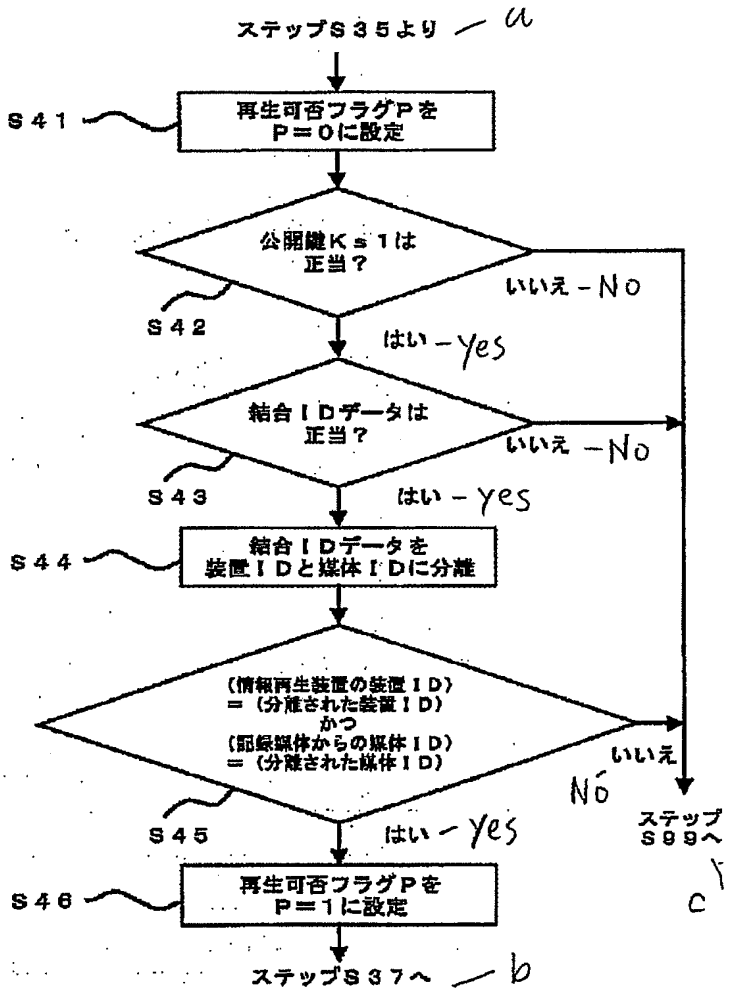
S99: Prohibit decoding of content

a: Permitted

b: Prohibited

c: End

FIG. 7



a: From Step S35

S41: Set flag P indicating whether to permit reproduction to be P = 0

S42: Public key Ks1 is authorized?

S43: Concatenated ID data is authorized?

S44: Separate concatenated ID data into apparatus ID and medium ID

S45: (apparatus ID of information reproducing apparatus = separated apparatus ID) and (medium ID of recording medium = separated medium ID)

S46: Set flag P indicating whether to permit reproduction to be P = 1

b: To Step S37

c: To Step S99

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－132457
（P2002－132457A）
(43)公開日　平成14年５月10日(2002.5.10)

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
G06F	3/06	304	G06F	3/06	304M　5B017
	12/14	320		12/14	320E　5B065
G09C	1/00	640	G09C	1/00	640B　5C053
G11B	20/10		G11B	20/10	H　5D044
H04N	5/91		H04N	5/91	P　5J104

審査請求　未請求　請求項の数12　ＯＬ　（全 17 頁）

(21)出願番号　特願2000－327591(P2000－327591)

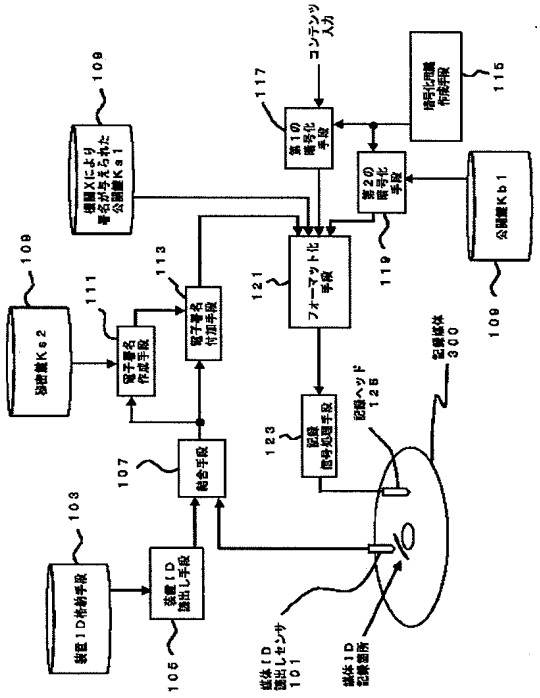
(22)出願日　平成12年10月26日(2000.10.26)

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地
(72)発明者　大石　剛士
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内
(74)代理人　100093067
弁理士　二瓶　正敬

最終頁に続く

(54)【発明の名称】　情報記録装置及び情報再生装置並びに情報記録再生装置

(57)【要約】
【課題】　コンテンツの記録が行われた情報記録装置の装置ＩＤが盗まれたり、不正に改変されたりした場合でも、１つの記録媒体から複製を行い、複数の複製された記録媒体を作成できないようにする。
【解決手段】　情報記録装置の装置ＩＤ格納手段１０３に格納されている、情報記録装置を識別可能とする装置ＩＤ又はその情報記録装置が属するグループＩＤと、記録媒体３００を識別可能とする媒体ＩＤとを結合した結合ＩＤデータに対して、電子署名付加手段１１３によって電子署名を付加し、このデータをコンテンツとともに記録媒体に記録する。これにより、情報再生装置がコンテンツを記録した情報記録装置と同一の装置又は再生可能なように設定されてグループに属している装置であり、さらにコンテンツが情報記録装置で記録された記録媒体と同一の記録媒体に記録されていると確認できた場合のみ、コンテンツの再生が可能となる。



1

【特許請求の範囲】

【請求項１】　記録媒体の識別を可能とする媒体ＩＤを有する前記記録媒体にデジタルデータを記録するものであり、他の装置からの識別を可能とする装置ＩＤ又は他のグループに属する装置からの識別を可能とするグループＩＤを有する情報記録装置であって、

前記記録媒体から前記媒体ＩＤを読み出す手段と、

前記情報記録装置から前記装置ＩＤ又は前記グループＩＤを読み出す手段と、

前記媒体ＩＤと前記装置ＩＤ又は前記グループＩＤとを結合して、結合ＩＤデータを作成する手段と、

前記結合ＩＤデータに電子署名を付加して、電子署名付き結合ＩＤデータを作成する手段と、

前記記録媒体に前記デジタルデータを記録する際、同時に前記電子署名付き結合ＩＤデータを前記記録媒体に記録する手段とを、

有する情報記録装置。

【請求項２】　前記デジタルデータに関連して前記デジタルデータの保護の度合いを示す再生制約情報が存在し、前記再生制約情報に基づいて前記デジタルデータの再生条件を指定する指定情報を作成する手段と、

前記デジタルデータの記録時に、同時に前記記録媒体に前記指定情報を記録する手段とを、

有することを特徴とする請求項１記載の情報記録装置。

【請求項３】　前記デジタルデータに関しては暗号化を行い、前記デジタルデータに付随する管理情報に関しては、すべての情報再生装置において読出し可能となるよう前記暗号化を行わないように制御することを特徴とする請求項１又は２記載の情報記録装置。

【請求項４】　前記記録媒体に前記デジタルデータを記録する前に、前記デジタルデータを暗号化し、前記デジタルデータの前記暗号化に用いられた暗号化用鍵を暗号化して、前記記録媒体に記録することを特徴とする請求項１ないし３のいずれか１つに記載の情報記録装置。

【請求項５】　デジタルデータと、前記デジタルデータを記録した情報記録装置の識別を可能とする装置ＩＤ又は前記情報記録装置が属するグループの識別を可能とするグループＩＤと前記デジタルデータが記録された記録媒体の識別を可能とする媒体ＩＤとが結合されて電子署名が付加された電子署名付き結合ＩＤデータとが記録された前記記録媒体から、前記デジタルデータを再生するものであり、他の装置からの識別を可能とする装置ＩＤ又は他のグループに属する装置からの識別を可能とするグループＩＤを有する情報再生装置であって、

前記記録媒体から前記媒体ＩＤを読み出す読出し手段と、

前記記録媒体から前記デジタルデータと前記電子署名付き結合ＩＤデータを読み出す手段と、

前記電子署名付き結合ＩＤデータに付加された電子署名を検証する第１の検証手段と、

2

前記電子署名付き結合ＩＤデータから前記媒体ＩＤと前記装置ＩＤ又は前記グループＩＤとを抽出する抽出手段と、

前記情報再生装置が有する前記装置ＩＤ又は前記グループＩＤと前記抽出手段によって抽出された前記装置ＩＤ又は前記グループＩＤとが一致するか否かを検証する第２の検証手段と、

前記読出し手段によって読み出された前記媒体ＩＤと前記抽出手段によって抽出された前記媒体ＩＤとが一致するか否かを検証する第３の検証手段と、

前記第１から第３の検証手段による検証のうちのいずれか１つの検証結果が正しくない場合には、前記デジタルデータの再生を不可とする手段とを、

有する情報再生装置。

【請求項６】　前記記録媒体に記録されているデータから、前記デジタルデータに関連して前記デジタルデータの保護の度合いを示す再生制約情報を読み出し、前記再生制約情報に応じて前記デジタルデータの再生条件を設定する手段を有することを特徴とする請求項５記載の情報再生装置。

【請求項７】　前記記録媒体に記録されているデータから、前記デジタルデータに付随する管理情報のみを読み出して、前記管理情報のみの出力を可能とすることを特徴とする請求項５又は６記載の情報再生装置。

【請求項８】　前記デジタルデータが暗号化されており、さらに前記暗号化に用いられた暗号化用鍵が暗号化されて前記記録媒体に記録されている場合、

前記記録媒体から読み出されたデータから前記暗号化用鍵を抽出し、前記情報再生装置が有する秘密鍵を用いて前記暗号化用鍵を復号し、前記復号された前記暗号化用鍵を用いて前記デジタルデータを復号することを特徴とする請求項５ないし７のいずれか１つに記載の情報再生装置。

【請求項９】　記録媒体の識別を可能とする媒体ＩＤを有する前記記録媒体にデジタルデータを記録し、前記記録媒体から前記デジタルデータを再生するものであり、他の装置からの識別を可能とする装置ＩＤを有する情報記録再生装置であって、

前記記録媒体に前記デジタルデータを記録するために、

前記記録媒体から前記媒体ＩＤを読み出す手段と、

前記情報記録装置から前記装置ＩＤを読み出す手段と、

前記媒体ＩＤと前記装置ＩＤとを結合して、結合ＩＤデータを作成する手段と、

前記結合ＩＤデータに電子署名を付加して、電子署名付き結合ＩＤデータを作成する手段と、

前記記録媒体に前記デジタルデータを記録する際、同時に前記電子署名付き結合ＩＤデータを前記記録媒体に記録する手段とを有し、

前記記録媒体から前記デジタルデータを再生するために、

前記記録媒体から前記媒体ＩＤを読み出す読出し手段と、
前記記録媒体から前記デジタルデータと前記電子署名付き結合ＩＤデータを読み出す手段と、
前記電子署名付き結合ＩＤデータに付加された電子署名を検証する第１の検証手段と、
前記電子署名付き結合ＩＤデータから前記媒体ＩＤと前記装置ＩＤとを抽出する抽出手段と、
前記情報再生装置が有する前記装置ＩＤと前記抽出手段によって抽出された前記装置ＩＤとが一致するか否かを検証する第２の検証手段と、
前記読出し手段によって読み出された前記媒体ＩＤと前記抽出手段によって抽出された前記媒体ＩＤとが一致するか否かを検証する第３の検証手段と、
前記第１から第３の検証手段による検証のうちのいずれか１つの検証結果が正しくない場合には、前記デジタルデータの再生を不可とする手段とを、
有する情報記録再生装置。

【請求項１０】　前記デジタルデータに関連して前記デジタルデータの保護の度合いを示す再生制約情報が存在し、
前記記録媒体に前記デジタルデータを記録する際に、
前記再生制約情報に基づいて前記デジタルデータの再生条件を指定する指定情報を作成し、前記デジタルデータの記録時に、同時に前記記録媒体に前記指定情報を記録し、
前記記録媒体から前記デジタルデータを再生する際に、
前記記録媒体に記録されているデータから、前記デジタルデータに関連して前記デジタルデータの保護の度合いを示す再生制約情報を読み出し、前記再生制約情報に応じて前記デジタルデータの再生条件を設定することを特徴とする請求項９記載の情報記録再生装置。

【請求項１１】　前記記録媒体に前記デジタルデータを記録する際に、
前記デジタルデータに関しては暗号化を行い、前記デジタルデータに付随する管理情報に関しては、すべての情報再生装置において読出し可能となるよう前記暗号化を行わないように制御して、
前記記録媒体から前記デジタルデータを再生する際に、
前記記録媒体に記録されているデータから、前記デジタルデータに付随する管理情報のみを読み出して、前記管理情報のみの出力を可能とすることを特徴とする請求項９又は１０記載の情報記録再生装置。

【請求項１２】　前記記録媒体に前記デジタルデータを記録する際に、
前記記録媒体に前記デジタルデータを記録する前に、前記デジタルデータを暗号化し、前記デジタルデータの前記暗号化に用いられた暗号化用鍵を暗号化して前記記録媒体に記録して、
前記記録媒体から前記デジタルデータを再生する際に、
前記記録媒体から読み出されたデータから前記暗号化用鍵を抽出し、前記情報再生装置が有する秘密鍵を用いて前記暗号化用鍵を復号し、前記復号された前記暗号化用鍵を用いて前記デジタルデータを復号することを特徴とする請求項９ないし１１のいずれか１つに記載の情報記録再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、放送又は通信ネットワークを介して映像及び／又は音声のコンテンツについて、不正な複製や改変が行われないようコンテンツを保護するための情報記録装置及び情報再生装置並びに情報記録再生装置に関し、特に、特定の装置でコンテンツの再生を可能とするものに関する。

【０００２】

【従来の技術】従来、特に画質や音質の劣化なくコンテンツ（デジタルデータ）の複製が可能な記録においては、コンテンツの著作権の保護が課題となっていた。そこで、コンテンツに複製を制御するための信号（付加情報）を付加し、記録装置では必ずこの付加情報を参照して記録を制御するように取り決めることにより不法コピーを防止する技術や、機器間の伝送において、コンテンツに対して暗号化を行うことにより、伝送の途中の信号を盗み見てコンテンツを不法に取得及び利用することを防止する技術が提案されてきた。これらの技術は、著作権が存在するコンテンツが他の記録媒体に記録されることを禁止することで、不法コピーが行われて記録された記録媒体が作成されることを防止するものである。

【０００３】また、例えばコンテンツを供給する従来の代表的な方法は、コンパクトディスク（ＣＤ）、デジタルビデオディスク（ＤＶＤ）などのディスク記録媒体やビデオソフトテープなどの磁気記録媒体にコンテンツを記録して、その記録媒体を販売する形態である。この場合、コンテンツが記録された記録媒体と同種の記録媒体の再生が可能な再生装置であれば、どの装置でもその記録媒体の再生が可能であり、購入者は自宅の再生装置で記録媒体を再生して、コンテンツを楽しむことができる。

【０００４】また、従来、コンテンツとともに装置ＩＤを記録してどの情報記録装置でコンテンツの記録が行われたかという記録を記録媒体中に残す方法も存在する。これにより、コンテンツを記録した情報記録装置に対応付けられた情報再生装置のみで、コンテンツの再生が可能となるようにすることができる。

【０００５】

【発明が解決しようとする課題】しかし、著作権保護に関する上記の従来技術は、基本的に記録媒体を販売する従来型の形態に対応したものであり、コンテンツが記録された記録媒体は、その種類の記録媒体の再生が可能な情報再生装置であれば、どの情報再生装置でも再生可能

なものである。そのため、特定の記録媒体に記録されたコンテンツが特定の装置でのみ再生できるようにすることはできない。

【０００６】また、コンテンツとともに装置ＩＤを記録してどの情報記録装置でコンテンツの記録が行われたかという記録を記録媒体中に残す方法に関しては、コンテンツの記録が行われた情報記録装置や不正に装置ＩＤが改変された情報記録装置を用いれば、１つの記録媒体から複製を行い、複数の複製された記録媒体（デッドコピー）を作成することが可能である。この場合、例えばコンテンツを記録媒体に記録した情報記録装置の装置ＩＤが不正に読み出されたり改変されたりした場合には、不正に改造された情報再生装置を用いて、簡単にコンテンツの不正な複製が可能となってしまう。

【０００７】本発明は、上記問題点に鑑み、情報再生装置がコンテンツを記録した情報記録装置と同一の装置又は再生可能なように設定されてグループに属している装置であり、さらにコンテンツが情報記録装置で記録された記録媒体と同一の記録媒体に記録されていると確認できた場合のみ、コンテンツの再生を可能とすることを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成するため、本発明は、コンテンツの記録の際に、そのコンテンツを記録する情報記録装置を識別可能とする装置ＩＤ又はその装置が属するグループを識別するグループＩＤと、そのコンテンツが記録されている記録媒体を識別可能とする媒体ＩＤとを、コンテンツとともに記録媒体に記録する。また、コンテンツの再生の際に、記録媒体に記録されている装置ＩＤ又はグループＩＤと媒体ＩＤとを参照して、コンテンツの再生が可能か否かを判定する。

【０００９】すなわち、本発明によれば、記録媒体の識別を可能とする媒体ＩＤを有する前記記録媒体にデジタルデータを記録するものであり、他の装置からの識別を可能とする装置ＩＤ又は他のグループに属する装置からの識別を可能とするグループＩＤを有する情報記録装置であって、前記記録媒体から前記媒体ＩＤを読み出す手段と、前記情報記録装置から前記装置ＩＤ又は前記グループＩＤを読み出す手段と、前記媒体ＩＤと前記装置ＩＤ又は前記グループＩＤとを結合して、結合ＩＤデータを作成する手段と、前記結合ＩＤデータに電子署名を付加して、電子署名付き結合ＩＤデータを作成する手段と、前記記録媒体に前記デジタルデータを記録する際、同時に前記電子署名付き結合ＩＤデータを前記記録媒体に記録する手段とを、有する情報記録装置が提供される。

【００１０】また、本発明によれば、デジタルデータと、前記デジタルデータを記録した情報記録装置の識別を可能とする装置ＩＤ又は前記情報記録装置が属するグループの識別を可能とするグループＩＤと前記デジタルデータが記録された記録媒体の識別を可能とする媒体ＩＤとが結合されて電子署名が付加された電子署名付き結合ＩＤデータとが記録された前記記録媒体から、前記デジタルデータを再生するものであり、他の装置からの識別を可能とする装置ＩＤ又は他のグループに属する装置からの識別を可能とするグループＩＤを有する情報再生装置であって、前記記録媒体から前記媒体ＩＤを読み出す読出し手段と、前記記録媒体から前記デジタルデータと前記電子署名付き結合ＩＤデータを読み出す手段と、前記電子署名付き結合ＩＤデータに付加された電子署名を検証する第１の検証手段と、前記電子署名付き結合ＩＤデータから前記媒体ＩＤと前記装置ＩＤ又は前記グループＩＤとを抽出する抽出手段と、前記情報再生装置が有する前記装置ＩＤ又は前記グループＩＤと前記抽出手段によって抽出された前記装置ＩＤ又は前記グループＩＤとが一致するか否かを検証する第２の検証手段と、前記読出し手段によって読み出された前記媒体ＩＤと前記抽出手段によって抽出された前記媒体ＩＤとが一致するか否かを検証する第３の検証手段と、前記第１から第３の検証手段による検証のうちのいずれか１つの検証結果が正しくない場合には、前記デジタルデータの再生を不可とする手段とを、有する情報再生装置が提供される。

【００１１】また、本発明によれば、記録媒体の識別を可能とする媒体ＩＤを有する前記記録媒体にデジタルデータを記録し、前記記録媒体から前記デジタルデータを再生するものであり、他の装置からの識別を可能とする装置ＩＤを有する情報記録再生装置であって、前記記録媒体に前記デジタルデータを記録するために、前記記録媒体から前記媒体ＩＤを読み出す手段と、前記情報記録装置から前記装置ＩＤを読み出す手段と、前記媒体ＩＤと前記装置ＩＤとを結合して、結合ＩＤデータを作成する手段と、前記結合ＩＤデータに電子署名を付加して、電子署名付き結合ＩＤデータを作成する手段と、前記記録媒体に前記デジタルデータを記録する際、同時に前記電子署名付き結合ＩＤデータを前記記録媒体に記録する手段とを有し、前記記録媒体から前記デジタルデータを再生するために、前記記録媒体から前記媒体ＩＤを読み出す読出し手段と、前記記録媒体から前記デジタルデータと前記電子署名付き結合ＩＤデータを読み出す手段と、前記電子署名付き結合ＩＤデータに付加された電子署名を検証する第１の検証手段と、前記電子署名付き結合ＩＤデータから前記媒体ＩＤと前記装置ＩＤとを抽出する抽出手段と、前記情報再生装置が有する前記装置ＩＤと前記抽出手段によって抽出された前記装置ＩＤとが一致するか否かを検証する第２の検証手段と、前記読出し手段によって読み出された前記媒体ＩＤと前記抽出手段によって抽出された前記媒体ＩＤとが一致するか否かを検証する第３の検証手段と、前記第１から第３の検証手段による検証のうちのいずれか１つの検証結果が正し

くない場合には、前記デジタルデータの再生を不可とする手段とを、有する情報記録再生装置が提供される。

【００１２】

【発明の実施の形態】以下、図面を参照しながら、本発明の情報記録装置及び情報再生装置並びに情報記録再生装置について説明する。まず、情報再生装置がそのコンテンツを記録した情報記録装置と同一のものであり（すなわち、情報再生装置と情報記録装置が同一かつ一体化している情報記録再生装置）、さらに情報記録装置で記録された記録媒体と同一の記録媒体（すなわち、別の場所でデータが複製されて記録された記録媒体を排除する）の場合のみ再生可能とする場合を説明する。

【００１３】図１は、本発明の情報記録装置に係る一実施形態を示す模式図である。情報記録装置（情報記録再生装置の記録系）は、媒体ＩＤ読出しセンサ１０１、装置ＩＤ格納手段１０３、装置ＩＤ読出し手段１０５、結合手段１０７、鍵格納手段１０９、電子署名作成手段１１１、電子署名付加手段１１３、暗号化用鍵作成手段１１５、第１の暗号化手段１１７、第２の暗号化手段１１９、フォーマット化手段１２１、記録信号処理手段１２３、記録ヘッド１２５により構成されている。また、記録媒体３００は、媒体ＩＤ読出しセンサ１０１及び記録ヘッド１２５が情報の読出し及び記録可能な位置に設置される。

【００１４】媒体ＩＤ読出しセンサ１０１は、記録媒体３００上にあらかじめ記録された媒体ＩＤを読み出すための手段である。この媒体ＩＤは、個々の記録媒体３００に与えられた記録媒体３００を識別するための識別情報であり、いったん記録媒体３００に記録されると追記や消去、変更が不可能な識別情報である。媒体ＩＤを記録媒体３００に記録する方法としては、例えば特開２０００－１０００６８号公報に記載されているように、ディスクの「バースト・カッティング・エリア」に記録する方法がある。これは記録媒体３００の製造時に、記録媒体３００に強力なレーザで媒体ＩＤを記録するもので、一般ユーザによる改変はほぼ不可能である。

【００１５】また、記録媒体３００が半導体メモリである場合には、例えば情報を読み出そうとするとその情報が消えてしまうようなヒューザブルなエリアが情報記録領域とは別途用意され、この領域に媒体ＩＤを記録することにより改変不可能にしたり、磁気ディスクに対して媒体ＩＤ記録用に書換え不可能なメモリを追加したりするなどの方法が考えられる。ここで、媒体ＩＤの格納個所が書換え不可能なメモリの場合には、媒体ＩＤ読出し手段には図１のようなセンサを用いず、そのメモリのＩＤが格納されているアドレスを読み出すことにより、媒体ＩＤの読出しが行われる。

【００１６】装置ＩＤ格納手段１０３は、この情報記録装置内部にあらかじめ装置ＩＤを格納しておくための手段である。この装置ＩＤは、個々の情報記録装置に与えられた情報記録装置を識別するための識別情報であり、この情報記録装置内部のメモリやハードウェアそのものに記録されるなど、情報記録装置の外部からは読出し不可能であり、いったん情報記録装置に記録されると追記や消去、変更が不可能な識別情報である。装置ＩＤ読出し手段１０５は、この装置ＩＤを読み出すことが可能な手段である。

【００１７】結合手段１０７は、媒体ＩＤ読出しセンサ１０１によって読み出された媒体ＩＤ、装置ＩＤ読出し手段１０５によって読み出された装置ＩＤの２つのデータを結合して、１つの結合ＩＤデータを作成する手段である。２つのデータの結合方法は、単に２つのデータを並べて１つの結合ＩＤデータを作成する方法、２つのデータを所定の順序に並べて１つの結合ＩＤデータを作成する方法、２つのデータに所定の演算を施して１つの結合ＩＤデータを作成する方法など、どのような結合方法でも可能である。

【００１８】鍵格納手段１０９は、秘密鍵Ｋｓ２、公開鍵Ｋｂ１、鍵の管理を行う機関Ｘにより署名が与えられた公開鍵Ｋｓ１（電子署名付き公開鍵Ｋｓ１）を格納するための手段である。図１では便宜上、それぞれの秘密鍵又は公開鍵に対して鍵格納手段が図示されているが、それぞれの鍵を格納する格納手段を設置することも可能であり、秘密鍵及び公開鍵をまとめて１つの格納手段に格納することも可能である。また、特に秘密鍵は情報記録装置外部から読出し不可能なように管理されて格納される必要があり、例えば、秘密鍵と公開鍵の格納手段をそれぞれ別々に設けて格納することも可能である。

【００１９】秘密鍵Ｋｓ２とペアになる公開鍵Ｋｓ１には、各装置を管理している所定の機関Ｘにより、同機関Ｘが持っていて決して外部へは出さない秘密鍵Ｋｓ２を用いて作成された電子署名があらかじめ付加されている。また、この電子署名を公開鍵Ｋｓ１とこの装置ＩＤを結合したデータとに対して作成するようにすることにより、公開鍵Ｋｓ１が他の装置で盗用された場合でも装置ＩＤが異なっているので、盗用の発見が容易になる。

【００２０】なお、一般にある秘密鍵で作成された電子署名が付加された情報は、その受信側または再生側で、受信または再生された電子署名が付加された情報に対して、その秘密鍵とペアとなる公開鍵を作用させて、所定の演算を施すことにより、受信または再生に至る途中のどこかで情報内容が改ざんされていないかを検証することが可能となる。その方法として、例えば文献N. Kovlitz, "Elliptic curvecriptosystems," Mathematics of Computation 48 (1987)203-209に記載されているＥＣＳＰ－ＤＳＡ (Elliptic Curve Signature Primitive,DSA version.)といった技術を用いればよい。

【００２１】電子署名作成手段１１１は、秘密鍵Ｋｓ２を用いて電子署名を作成する手段である。電子署名付加手段１１３は、結合手段１０７によって作成された結合

ＩＤデータに、電子署名作成手段１１１によって作成された電子署名を付加する手段である。暗号化用鍵作成手段１１５は、入力されたコンテンツを暗号化するための暗号化用鍵Ｋａを作成する手段であり、例えば暗号化用鍵となる乱数を発生させる乱数発生手段を用いることができる。この暗号化用鍵Ｋａは、各コンテンツに応じて、毎回異なる暗号化用鍵を作成する。第１の暗号化手段１１７は、暗号化用鍵作成手段１１５によって作成された暗号用鍵を用いて、入力されたコンテンツデータを暗号化する手段である。第２の暗号化手段１１９は、公開鍵Ｋｂ１を用いて暗号化用鍵作成手段１１５によって作成された暗号化用鍵を暗号化する手段である。なお、コンテンツは例えばデジタル放送などの放送ネットワークやインターネットなどの通信ネットワークを介して情報記録装置外部から配信されるものである。

【００２２】フォーマット化手段１２１は、電子署名が付加された結合ＩＤデータ、第１の暗号化手段によって暗号化されたコンテンツ、第２の暗号化手段によって暗号化された鍵Ｋａ、機関Ｘにより署名が与えられた公開鍵Ｋｓ１（電子署名付き公開鍵Ｋｓ１）を結合し、フォーマット化して１つのデータとする手段である。記録信号処理手段１２３は、フォーマット化手段１２１によって作成された１つのデータを記録媒体３００に記録可能となる信号に、例えば記録変調処理などの変換処理を行う手段である。記録ヘッド１２５は、記録信号処理手段１２３によって処理された信号を記録媒体３００に記録するための手段である。

【００２３】次に、図１に示す本発明の情報記録装置に係る記録媒体にコンテンツを記録する動作について説明する。図３及び図４は、本発明の情報記録装置に係る処理動作の一例を示すフローチャートの１枚目及び２枚目である。なお、図３及び図４は図中の「Ａ」と示された箇所でつながっている。

【００２４】まず、ステップＳ１１において、装置ＩＤ読出し手段１０５が、装置ＩＤ格納手段１０３からその情報記録装置を識別する装置ＩＤを読み出す。一方、ステップＳ１２において、媒体ＩＤ読出しセンサ１０１が、記録媒体３００からその記録媒体３００を識別する媒体ＩＤを読み出す。ステップＳ１３において、結合手段１０７が、これらの媒体ＩＤと装置ＩＤの２つのデータを結合して、１つの結合ＩＤデータを作成する。ステップＳ１４において、電子署名作成手段１１１が、ステップＳ１３で作成された結合ＩＤデータと鍵格納手段１０９に格納された秘密鍵Ｋｓ２とを用いて、結合ＩＤデータに対する電子署名を作成する。ステップＳ１５において、電子署名付加手段１１３が、ステップＳ１４で作成された電子署名を結合ＩＤデータに付加する。

【００２５】ステップＳ１６において、暗号化用鍵作成手段１１５がコンテンツを暗号化するための暗号化用鍵Ｋａを作成する。ステップＳ１７において、第１の暗号化手段１１７が、ステップＳ１６で作成された暗号化用鍵Ｋａを用いて、情報記録装置に入力されたコンテンツを暗号化する。一方、ステップＳ１８において、ステップＳ１６で作成された暗号化用鍵Ｋａは第２の暗号化手段１１９にも入力されて、第２の暗号化手段１１９が、公開鍵Ｋｂ１を用いて暗号化用鍵Ｋａを暗号化する。

【００２６】そして、ステップＳ１３で作成された電子署名が付加された結合ＩＤデータ、ステップＳ１７で暗号化されたコンテンツ、ステップＳ１８で暗号化された暗号化用鍵Ｋａ、機関Ｘにより署名が与えられた電子署名付き公開鍵Ｋｓ１がフォーマット化手段１２１に入力されて、ステップＳ１９において、フォーマット化手段１２１が、これらのデータ（電子署名付き結合ＩＤデータ、暗号化されたコンテンツ、暗号化された暗号化用鍵Ｋａ、電子署名付き公開鍵Ｋｓ１）をフォーマット化して１つのデータとする。このとき、フォーマット化手段１２１は、これらのデータをそれぞれ所定のフォーマットの中の所定の場所に挿入する。

【００２７】なお、この電子署名付き結合ＩＤデータ、暗号化された暗号化用鍵Ｋａ、電子署名付き公開鍵Ｋｓ１をコンテンツの記録に付随したサブコードエリアやＡＵＸエリアに挿入したり、コンテンツに関連付けられた別のファイルとしたり、記録媒体３００に記録されたコンテンツを一括管理する一覧表のデータとして記録したりすることも可能である。また、このフォーマット化の際に、フォーマット化手段によって作成されたフォーマット化データには誤り訂正符号が付加されることが好ましい。

【００２８】ステップＳ２０において、記録信号処理手段１２３が、フォーマット化データに対して記録変調処理などの記録信号処理を行う。ステップＳ２１において、記録ヘッド１２５を用いて、ステップＳ２０で処理された信号を記録媒体３００に記録する。なお、記録媒体３００が半導体の場合には記録変調処理は省略されるなど、記録媒体３００の性質に適した方法で信号が記録される。

【００２９】次に、コンテンツ情報の記録媒体３００からの再生時の動作を説明する。図２は、本発明の情報再生装置に係る一実施形態を示す模式図である。情報再生装置（情報記録再生装置の再生系）は、媒体ＩＤ読出しセンサ２０１、装置ＩＤ格納手段２０３、装置ＩＤ読出し手段２０５、再生ヘッド２０７、再生信号処理手段２０９、データ抽出手段２１１、鍵格納手段２１３、再生可否判定手段２１５、第１の復号手段２１７、第２の復号手段２１９、制御手段２２１により構成されている。また、記録媒体３００は、媒体ＩＤ読出しセンサ２０１及び再生ヘッド２０７が情報の読出し可能な位置に設置される。

【００３０】媒体ＩＤ読出しセンサ２０１は、記録媒体３００上にあらかじめ記録された媒体ＩＤを読み出すた

めの手段である。装置ＩＤ格納手段２０３は、この情報再生装置内部にあらかじめ装置ＩＤを格納しておくための手段である。この装置ＩＤは、個々の情報再生装置に与えられた情報再生装置を識別するための識別情報であり、この情報再生装置内部のメモリやハードウェアそのものに記録されるなど、情報再生装置の外部からは読出し不可能となるように記録されている。装置ＩＤ読出し手段２０５は、この装置ＩＤを読み出すことが可能な手段である。

【００３１】再生ヘッド２０７は、記録媒体３００に記録された信号を読み出すための手段である。再生信号処理手段２０９は、再生ヘッドで読み出された信号を処理可能なデータに変換処理する手段である。データ抽出手段２１１は、再生信号処理手段２０９で処理されたデータに含まれている各データを選別及び抽出する手段である。鍵格納手段２１３は、公開鍵Ｋｘ１、秘密鍵Ｋｂ２を格納するための手段である。なお、図１と同様に、図２でも便宜上、それぞれの秘密鍵又は公開鍵に対して鍵格納手段２１３が図示されているが、秘密鍵及び公開鍵を１つの格納手段で行うことも可能であり、また、複数の格納手段を用いることも可能である。また、秘密鍵は情報再生装置外部から読出し不可能なように管理されて格納される必要がある。

【００３２】再生可否判定手段２１５は、装置ＩＤ、媒体ＩＤ、電子署名付きＫｓ１、電子署名結合ＩＤデータなどを参照して、コンテンツの再生を可能とするか否かを判定し、その結果、例えばメモリなどの所定のアドレスに存在する再生可否フラグＰをＰ＝１（再生可能）とする処理を行う手段である。第１の復号手段２１７は、暗号化されたコンテンツを暗号用鍵Ｋａを用いて、復号する手段である。なお、暗号化用鍵Ｋａは、コンテンツの暗号化の際に用いられた鍵であり、コンテンツを復号する場合、復号用鍵として用いられる。

【００３３】第２の復号手段２１９は、暗号化された暗号化用鍵Ｋａを、秘密鍵Ｋｂ２を用いて復号する手段であり、これによって、第１の復号手段２１７で用いられる暗号化用鍵Ｋａが出力される。制御手段２２１は、再生可否判定手段２１５によって出力される結果（再生可否フラグＰがＰ＝０かＰ＝１）に応じて、第１の復号手段２１７によるコンテンツの復号の動作を制御する手段である。なお、媒体ＩＤ読出しセンサ２０１、装置ＩＤ格納手段２０３、装置ＩＤ読出し手段２０５、鍵格納手段２１３は、それぞれ媒体ＩＤ読出しセンサ１０１、装置ＩＤ格納手段１０３、装置ＩＤ読出し手段１０５、鍵格納手段１０９と同じ機能を有する。

【００３４】次に、図２に示す本発明の情報記録装置に係る記録媒体３００に記録されたコンテンツを再生する動作について説明する。図５及び図６は、本発明の情報再生装置に係る処理動作の一例を示すフローチャートの１枚目及び２枚目である。なお、図５及び図６は図中の「Ｂ」と示された箇所でつながっている。まず、ステップＳ３１において、装置ＩＤ読出し手段２０５が、装置ＩＤ格納手段２０３からその情報再生装置を識別する装置ＩＤを読み出す。

【００３５】一方、ステップＳ３２において、媒体ＩＤ読出しセンサ２０１が、記録媒体３００からその記録媒体３００を識別する媒体ＩＤを読み出し、ステップＳ３３において、再生ヘッドが、記録媒体３００に記録された信号を読み出す。なお、記録媒体３００が半導体の場合には、媒体ＩＤ読出しセンサ２０１や再生ヘッド２０７を用いるのではなく、該当するアドレスの読出しを行うなどの記録媒体３００に応じた処理が行われる。ステップＳ３４において、再生信号処理手段２０９が、ステップＳ３３で読み出された信号を処理可能なデータに変換処理する。ステップＳ３５において、データ抽出手段２１１が、ステップＳ３４で処理されたデータから、電子署名付き結合ＩＤデータ、暗号化されたコンテンツ、暗号化された暗号化用鍵Ｋａ、電子署名付き公開鍵Ｋｓ１を抽出する。

【００３６】ステップＳ３６において、再生可否判定手段が２１５が、ステップＳ３５で抽出された電子署名付き結合ＩＤデータ、電子署名付き公開鍵Ｋｓ１、装置ＩＤ、媒体ＩＤを参照して、コンテンツの再生（コンテンツの復号）が可能か否かを判定する。このステップＳ３６における再生可否の判定や、再生の可否を示す再生可否フラグＰに関しては、後で詳細に説明する。

【００３７】ステップＳ３６でコンテンツの復号が可能と判定された場合、再生可否フラグＰが再生可能であることを示すＰ＝１に設定される。ステップＳ３７において、秘密鍵Ｋｂ２を用いて、第２の復号手段２１９がステップＳ３５で抽出された暗号化された暗号化用鍵Ｋａを復号し、さらにステップＳ３８において、復号された鍵Ｋａを用いて、第１の復号手段２１７が暗号化されたコンテンツを復号する。

【００３８】一方、ステップＳ３６でコンテンツの復号が不可能と判定された場合、ステップＳ９９において、コンテンツの復号を禁止する。こうして得た判定結果により、Ｐ＝１のときのみコンテンツ情報の再生を行い、例えば制御手段２２１が第１の復号手段によるコンテンツの復号の動作を制御して、コンテンツの復号が行われないようにする。また、制御手段２２１が、第２の復号手段２１９による暗号化鍵Ｋａの復号の動作を制御して、暗号化鍵Ｋａが復号されないようにし、その結果、コンテンツの復号が行われないようにすることも可能である。

【００３９】次に、ステップＳ３６におけるコンテンツの再生可否の判定に関して、詳細に説明する。図７は、図６に示すフローチャートのステップＳ３６におけるコンテンツの再生可否の判定の動作の一例を示すフローチャートである。この再生可否に係る動作は、情報再生装

置のマイコンが適宜必要なデータを情報再生装置のマイコン内のメモリに取り込んで行うものである。ステップＳ３５の後、まず、ステップＳ４１において、再生可否フラグＰを初期化して、Ｐ＝０と設定する。ここで再生可否判定フラグＰは、Ｐ＝０のとき再生不可、Ｐ＝１のとき再生可を表すフラグであり、再生可否判定が終了していない段階では再生は不可（Ｐ＝０）とする。

【００４０】次に、ステップＳ４２において、電子署名付き公開鍵Ｋｓ１に対して、再生機器が機関Ｘから付与されて持っている公開鍵Ｋｘ１を用いて、公開鍵Ｋｓ１が正当なものか否かを判定する。公開鍵Ｋｓ１を保護している電子署名は機関Ｘ以外の者は知ることのできない秘密鍵Ｋｘ２により作成されているため、正しい電子署名を第三者が作成することはできない。したがって、第三者が、公開鍵Ｋｓ１と秘密鍵Ｋｓ２のペアを別のものに不正に入れ替えたとしても、この検証で正しくないと判定される。ステップＳ４２で公開鍵Ｋｓ１が正しくないと判定された場合、再生可否フラグはＰ＝０のまま、ステップＳ９９において判定を終了し、コンテンツの復号を禁止する。なお、電子署名が公開鍵Ｋｓ１と装置ＩＤとの結合データに対して施されている場合には、この結合データが正しく送られたことを検証することで、公開鍵Ｋｓ１そのものの改ざんの有無に加えて、確かにその装置のものであることが検証できる。

【００４１】ステップＳ４２の検証で公開鍵Ｋｓ１が正しいと判定された場合、ステップ４３において、電子署名付き結合ＩＤデータに対して、ステップＳ４２で正当なものであると判定された公開鍵Ｋｓ１を用いて、結合ＩＤデータが正当なものか否かを判定する。第三者が記録媒体３００内に記録された装置ＩＤと媒体ＩＤを不正に書き換えたとしても、この検証で正しくないと判定される。ステップＳ４３で結合ＩＤデータが正しくないと判定された場合、再生可否フラグはＰ＝０のまま、ステップＳ９９において判定を終了し、コンテンツの復号を禁止する。

【００４２】ステップＳ４３の検証で結合ＩＤデータが正しいと判定された場合、ステップＳ４４において、結合ＩＤデータを装置ＩＤと媒体ＩＤに分離する。次に、ステップＳ４５において、ステップＳ３１で読み出された情報再生装置の装置ＩＤ及びステップＳ３２で読み出された記録媒体３００の媒体ＩＤと、ステップＳ４４でＩＤ結合データから分離された装置ＩＤ及び媒体ＩＤとがそれぞれ等しいか否かを判定する。ステップＳ４５で装置ＩＤ及び媒体ＩＤの両方ともが等しい場合、ステップＳ４６において、再生可否フラグＰをＰ＝１とする。一方、両方又はどちらかが一方が等しくない場合、再生可否フラグはＰ＝０のまま、ステップＳ９９において判定を終了し、コンテンツの復号を禁止する。なお、この再生可否フラグＰがＰ＝１の場合には、コンテンツの再生が可能となり、Ｐ＝０の場合にはコンテンツの再生が不可能となるよう設定されている。

【００４３】以上の動作は、コンテンツ（番組）ごとに行われ、コンテンツに装置ＩＤ及び媒体ＩＤを関連させてコンテンツを記録するか否かを定めることが可能である。その結果、後述の再生動作により、あるコンテンツに関しては、同一の装置ＩＤを有さない情報再生装置では読出し不可能とし、別のコンテンツに関しては、すべての情報再生装置で読出し可能とすることができる。すなわち、１つの記録媒体３００に上記の動作による保護を受けたコンテンツと、保護のない一般的な記録条件で記録されたコンテンツとを共存させることが可能である。

【００４４】また、上記の実施の形態では、情報再生装置がそのコンテンツを記録した情報記録装置と同一のものであり、さらに情報記録装置で記録された記録媒体３００と同一の記録媒体３００の場合のみ再生可能とする場合について説明したが、情報再生装置がそのコンテンツを記録した情報記録装置と同一のグループに属するものであり、さらに情報記録装置で記録された記録媒体３００と同一の記録媒体３００の場合のみ再生可能とすることも可能である。

【００４５】ここで、同一のグループとは、情報記録装置と情報再生装置が同一の装置ではない場合でも、例えば同一のユーザが所有する複数の装置で構成するグループを特定するものである。例えばこのグループに属する情報再生装置に限って再生を許可するようにコンテンツを記録媒体３００に記録する場合、記録媒体３００にコンテンツとともにグループＩＤを記録する。そして、このグループ内の装置でグループＩＤを共有してそれぞれの装置内に格納しておき、記録媒体３００中のグループＩＤが情報再生装置に格納されたグループＩＤと一致した場合のみ情報再生装置でコンテンツの再生が可能となるようにすればよい。

【００４６】また、例えば各装置に装置ＩＤが割り当てられているが、このとき同時にどのグループに属するものかを示すグループＩＤも付加されることによって、各装置にグループＩＤを割り当てることが可能となる。例えば、セキュアーなデジタル出力と有効なコピープロテクション手段を持つ装置であるかどうかを示す情報が各装置の装置ＩＤとともに格納されており、特定の機関Ｘがその情報群に署名したものが各装置に格納されることによって、グループ化されることになる。

【００４７】このとき、装置ＩＤにグループＩＤが付加されているため、図１及び図２の装置ＩＤ格納手段は装置ＩＤ＋グループＩＤ格納手段と読み替えられ、図１及び図２の装置ＩＤ読出し手段は装置ＩＤ＋グループＩＤ格納手段と読み替えられる。また、図３～７に示すフローチャートでは、装置ＩＤは装置ＩＤ＋グループＩＤと読み替えられ、ステップＳ４５で装置ＩＤが一致するか否かを検証する代わりに、グループＩＤが一致するか否

かを検証することによって、同一のグループに属する装置がコンテンツの再生を行えるようにすることが可能となる。

【００４８】なお、再生されて出力されるコンテンツは、他の記録媒体３００に記録される可能性がある。これを防ぐために、理想的にはデスクランブルされた後のデータはその後デコードされ、最終的にＤ／Ａ変換されるまで一切ＬＳＩの外側に出なく、なおかつ、Ｄ／Ａ変換出力には有効なコピープロテクション手段がなされている必要がある。この構成が実現できない場合でも、信号が流れる箇所にはユーザが簡単には触れられない構成（例えばＢＧＡのＬＳＩのピンから基板の内層を通って別のＢＧＡのＬＳＩのピンに接続されるなどの構成）とすることも可能である。また、コンテンツの出力に関しては、さらに暗号化して出力することも可能である。また、上記実施の形態では、第１の暗号化手段によってコンテンツの暗号化を行っているが、コンテンツの保護の度合いは大きく弱まるものの、このコンテンツの暗号化を行わないことも可能である。

【００４９】さらに、コンテンツの供給者が、例えばコンテンツを記録媒体３００に記録した情報記録装置と同一の情報再生装置（すなわち１つの情報再生記録装置）のみでしかコンテンツの読出しが不可能、コンテンツを記録媒体３００に記録した情報記録装置と同一のグループに属する情報再生装置のみでしかコンテンツの読出しが不可能、どの情報再生装置でもコンテンツの読出しが可能などのコンテンツの保護条件を指定して、記録媒体３００に記録したい場合がある。この場合、コンテンツの供給者は、コンテンツの供給とともに記録再生条件を指定する付加情報も同時に供給する必要がある。

【００５０】また、管理情報とコンテンツとを分けて、管理情報に関しては暗号化が行われないようにしたい場合もある。この管理情報は、タイトル、記録時間などのコンテンツ中の番組の概要を示す情報を含んでいる。この管理情報が暗号化されずに直接読出し可能な形で記録媒体３００に記録されている場合、この管理情報を再生することにより、記録媒体３００にどのようなコンテンツが入っているか、どのくらいの容量を消費しているかなどの情報や、暗号化されている番組に関するタイトルや時間などの情報を簡単に利用することが可能となる。

【００５１】次に、上記のコンテンツの供給者からの付加情報を受けて、コンテンツとともに管理情報を記録する動作について説明する。図８は、本発明の情報記録装置に係るコンテンツとともに管理情報を記録する一実施形態を示す模式図である。情報記録装置は、媒体ＩＤ読出しセンサ１０１、装置ＩＤ格納手段１０３、装置ＩＤ読出し手段１０５、結合手段１０７、鍵格納手段１０９、電子署名作成手段１１１、電子署名付加手段１１３、暗号化用鍵作成手段１１５、第１の暗号化手段１１７、第２の暗号化手段１１９、フォーマット化手段１２１、記録信号処理手段１２３、記録ヘッド１２５、データ分離手段１２７、管理情報作成手段１２９、メモリ１３１、入力選択手段１３３により構成されている。また、記録媒体３００は、媒体ＩＤ読出しセンサ１０１及び記録ヘッド１２５が情報の読出し及び記録可能な位置に設置される。

【００５２】次に、図８の各手段の動作について説明する。なお、図８に示す手段のうち図１に示す手段と同一の手段に関しては同一の参照番号が付されており、必要でない場合には説明を省略する。フォーマット化手段１２１は、第１の暗号化手段１１７によって暗号化されたコンテンツをフォーマット化して１つのデータとする手段である。データ分離手段１２７は、ＭＰＥＧトランスポートストリームから付加情報とコンテンツとを分離する手段である。後述する再生制約フラグＱの値に応じて管理情報を作成する手段である。メモリ１３１は、管理情報を一時的に保存する手段である。入力選択手段１３３は、暗号化されたコンテンツと管理情報の出力を切り替えて、記録信号処理手段１２３に出力する手段である。

【００５３】次に、図８に示す本発明の情報記録装置に係るコンテンツとともに管理情報を記録する動作について説明する。図９は、本発明の情報記録装置に係るコンテンツとともに管理情報を記録する処理動作の一例を示すフローチャートである。例えば装置には、デジタル放送で使われているようなＭＰＥＧトランスポートストリームが入力されているものとする。

【００５４】まず、ステップＳ５１において、データ分離手段１２７が、ＭＰＥＧトランスポートストリームから付加情報とコンテンツとを分離し、その付加情報を抽出する。付加情報には、タイトル、記録時間などのコンテンツ管理情報が含まれている。さらに、付加情報には、ＭＰＥＧトランスポートストリームの作成の際に、コンテンツを再生する際の情報再生装置や記録媒体３００に関して、制約を行うか否かの情報である再生制約情報が作成者によって挿入されている。

【００５５】また、ＭＰＥＧトランスポートストリームでは、情報はパケットで送られており、そのＰＩＤ（パケットＩＤ）を参照することによって、そのパケットにどのようなデータが含まれているかがわかるようになっている。そして、コンテンツに含まれる番組に関して、どのＰＩＤを有するデータが映像データ、音声データ、付加情報データのうちのどのデータを有しているかは、番組選択の情報であるＰＭＴ（Program Map Table：番組対応表）というパケットに記述されて送信される。したがって、このＰＭＴを参照すれば、付加情報を抽出することが可能となる。

【００５６】ステップＳ５２において、ステップＳ５１で分離された付加情報から再生制約情報を読み出し、ステップＳ５３において、再生制約情報を参照して、同一

装置、同一の記録媒体３００に制約するよう指定されているか否かを判断する。この再生制約情報は、コンテンツの供給者又は作成者が決定した著作権の保護条件を示す情報である。同一装置、同一の記録媒体３００に制約するよう指定されていると判断された場合、ステップＳ５４において、再生制約フラグＱが、同一装置、同一の記録媒体３００に制約することを示すＱ＝１１に設定され、ステップＳ５５において、管理情報作成手段はＱ＝１１の値に応じて管理情報TypeIを作成する。

【００５７】一方、ステップＳ５３で同一装置、同一の記録媒体３００に制約するよう指定されていないと判断された場合、ステップＳ５６において、再生制約情報を参照して、同一グループ、同一の記録媒体３００に制約するよう指定されているか否かを判断する。同一グループ、同一の記録媒体３００に制約するよう指定されていると判断された場合、ステップＳ５７において、再生制約フラグＱが、同一グループ、同一の記録媒体３００に制約することを示すＱ＝１０に設定され、ステップＳ５８において、管理情報作成手段はＱ＝１０の値に応じて管理情報TypeIIを作成する。

【００５８】そして、ステップＳ５９において、ステップＳ５５で作成された管理情報TypeI又はステップＳ５８で作成された管理情報TypeIIをメモリに記憶する。さらに、ステップＳ６０において、第１の暗号化手段はコンテンツを暗号化し、暗号化されたコンテンツを記録媒体３００に記録する。

【００５９】一方、ステップＳ５６で同一グループ、同一の記録媒体３００に制約するよう指定されていないと判断された場合、ステップＳ６１において、再生制約フラグＱが装置の制約を行わないことを示すＱ＝００に設定され、ステップＳ６２において、管理情報作成手段は、Ｑ＝００の値に応じて管理情報TypeIIIを作成する。そして、ステップＳ６３において、ステップＳ６２で作成された管理情報TypeIIIをメモリに記憶する。ステップＳ６４において、第１の暗号化手段を制御して、コンテンツの暗号化が行われないようにして、コンテンツを記録媒体３００に記録する。その後、ステップＳ６５において、ステップＳ６２で作成された管理情報TypeIIIを記録媒体３００の管理情報エリアに記録する。

【００６０】なお、再生制約フラグＱの値に応じて、管理情報として入れなければならない情報が異なるので、再生制約フラグＱの値が異なれば、例えば管理情報の内容が異なったり、管理情報内に存在する情報の意味が異なったりする。以下に、この管理情報について説明する。図１０は、管理情報TypeI、管理情報TypeII、管理情報TypeIIIの一例を示す図である。なお、この実施の形態では、再生制約フラグＱ＝１１の場合には管理情報TypeI、再生制約フラグＱ＝１０の場合には管理情報TypeII、再生制約フラグＱ＝００の場合には管理情報TypeIIIが作成されるものとする。

【００６１】管理情報について、具体例としては、例えば図１０の（ａ）管理情報TypeI、（ｂ）管理情報TypeII、（ｃ）管理情報TypeIIIが考えられる。記録する各番組について、これらの管理情報が作成され、記録媒体３００内の管理情報エリアに記録される。管理情報には、番組番号、タイトル、信号仕様、記録仕様、記録位置情報、記録時間情報の６つのTypeI～IIIに共通した情報と、再生制約フラグＱ及び再生制約フラグＱの値に応じた様々な情報が含まれている。

【００６２】番組番号は、記録媒体３００に記録された番組を区別する整理番号である。タイトルは、入力されるＭＰＥＧトランスポートストリーム中の付加情報として送られてくるタイトル情報である。このタイトルに関しては、ユーザが情報記録装置において入力することも可能である。信号仕様は、コンテンツの転送レートや圧縮のパラメータなどの信号仕様のデータである。記録仕様は、記録において高品質モードと標準モードといった記録レートの違いや、音声のチャンネル数などについていくつかの仕様が有る場合、それらのうちのどの条件で記録したのかを示す情報である。

【００６３】また、記録位置情報は、例えば記録媒体３００が細かいセクターに分かれている時に、セクターのうちのどこからどこまでがこのコンテンツの記録に割り当てられているかを示す情報である。なお、ディスクの場合には記録するセクターは離れた位置に存在することも可能であり、書き込み可能なセクターが制御手段などによって選択される。記録時間情報は、このコンテンツの全記録時間を示す情報である。これらの記録位置及び時間情報はコンテンツの記録中に逐次更新され、コンテンツの記録が終了した時点での情報が管理情報として記録媒体３００に記録される。なお、途中でコンテンツの記録を中止したときは、それまでの記録時間が記録時間情報として記録される。以上が管理情報TypeI～IIIに共通した情報である。

【００６４】一方、再生制約フラグＱは、上記のフローチャートによって定められた再生時の制約を示すフラグであり、再生時の制約条件に従って異なる値となっている。この再生制約フラグＱは３つのタイプに分かれており、この値に応じて、この後に続くデータの有無やデータの意味などが異なってくる。

【００６５】図１０中の（ａ）に示す管理情報は、情報再生装置がそのコンテンツを記録した情報記録装置と同一のものであり、さらに情報記録装置で記録された記録媒体３００と同一の記録媒体３００の場合のみ再生可能とすることを示す再生制約フラグＱ＝１１を有するものである。この管理情報には、電子署名付き結合ＩＤデータ、公開鍵Ｋｓ１が含まれ、さらに、コンテンツが暗号化されるか否か（コンテンツの暗号化の有無）の情報が入り、コンテンツの暗号化が行われる場合には、管理情報には暗号化された暗号化用鍵Ｋａが含まれる。一方、

コンテンツが暗号化されない場合には、暗号化された暗号化用鍵Ｋａが入るべき項目には、例えばオール０などの所定のダミーデータが入れられるか、または、この項目が省略される規定とすることも可能である。

【００６６】一方、図１０中の（ｂ）に示す管理情報は、情報再生装置がそのコンテンツを記録した情報記録装置と同一のグループに属するものであり、さらに情報記録装置で記録された記録媒体３００と同一の記録媒体３００の場合のみ再生可能とすることを示す再生制約フラグＱ＝１０を有するものである。

【００６７】この場合、管理情報には機器グループ情報が追加される。ここで、機器グループ情報は、例えば機関Ｘが各機器に対して与えられる情報である。また、コンテンツを供給する側は、コンテンツの配信において、付加情報中にコンテンツの再生を認めるグループを指定しておき、その情報を機器グループ情報として記述しておく。そして、コンテンツを例えばＭＰＥＧトランスポートストリームに変換するときに、この機器グループ情報を付加情報としてコンテンツとともに記録し、この機器グループ情報を参照して再生を許可する機器のグループを図１０（ｂ）の機器グループ情報の項目に記述する。一方、再生の際には、この機器グループ情報の記述内容により、今再生しようとしている情報再生装置が再生が許可されたグループに属する場合のみ再生を行うようにする。

【００６８】一方、図１０中の（ｃ）に示す管理情報は、特に情報再生装置を制約せずに、すべての情報再生装置で再生可能とすることを示す再生制約フラグＱ＝００を有するものである。したがって、特に制約を設けないので、電子署名付き結合ＩＤデータ、公開鍵Ｋｓ１情報などは必要なく、それらの項目も設けられていない。一方、コンテンツを暗号化するか否かの選択が可能となるように、コンテンツの暗号化の有無の項目と、暗号化された暗号化用鍵Ｋａの項目が存在する。コンテンツを暗号化するか否かの選択は、コンテンツの供給者の付加情報による指定に従うようにすることが可能であるが、一般にはコンテンツの暗号化は行わないようにして、ユーザがそのコンテンツを他人に再生されたくない場合に、ユーザの指定により暗号化を行うような機能を情報記録装置に持たせることも可能である。

【００６９】また、図９に示すのフローチャートでは、管理情報を最後に記録媒体３００に記録しているが、コンテンツの記録に先立って記録可能な項目に関しては記録しておき、記録位置情報や記録時間情報などに関しては、コンテンツの記録に割り込む形で記録を更新していくようにすることも可能である。また、付加情報に記録される再生条件の指定は、個々の番組について行われるため、同一の記録媒体３００上に記録されている番組について再生条件を変えて記録することも可能であり、１つの記録媒体３００中に暗号化されている番組と暗号化されていない番組とを混在させることも可能である。

【００７０】次に、図９の情報記録装置で記録されたコンテンツ及び管理情報を再生する動作について説明する。図１１は、本発明の情報再生装置に係るコンテンツ及び管理情報が記録された記録媒体を再生する一実施形態を示す模式図である。なお、図１１を構成する手段は、図１を構成する手段と同一である。データ抽出手段によってコンテンツ及び管理情報が抽出され、コンテンツは図５及び図６のフローチャートに示す動作によって復号され、一方、管理情報は暗号化されていないので、そのまま出力することが可能である。

【００７１】すなわち、同一の装置でのみ再生することを許可するか否かの指定を示す付加情報が記録されている場合、再生時にはまずこの付加情報を読み出す。そして、この付加情報の内容によって、同一又は同一のグループの装置でのみ再生が許可されている場合には図５及び図６のフローチャートにおける判定に従って、再生処理を行う。一方、他の装置による再生も許可されている場合には、図５及び図６のフローチャートにおける判定処理は行わないか、または、同一媒体に記録された他のコンテンツの再生のために判定処理は行っても、このコンテンツに関しては判定結果にかかわらず再生を行う。また、コンテンツが暗号化されているか否かによって、暗号化されたコンテンツの復号処理を行うか否かの処理を切り替えることも可能である。

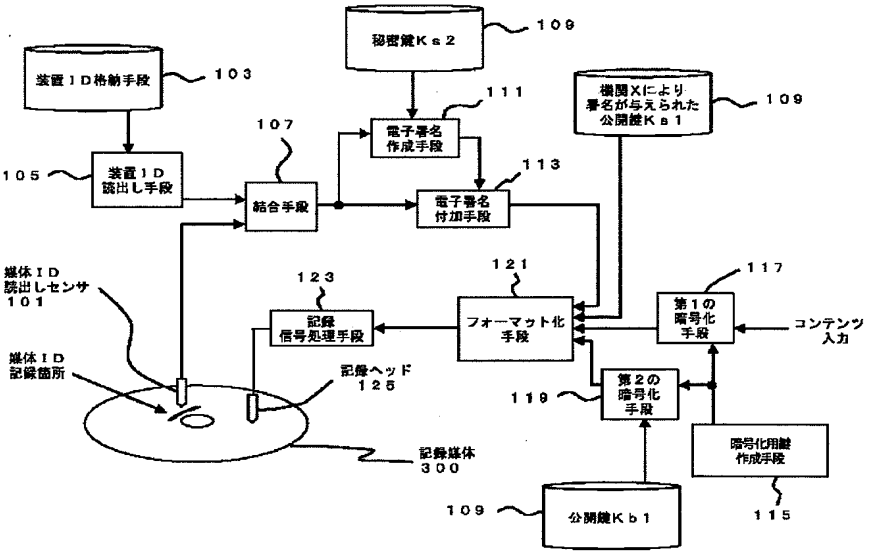
【００７２】また、タイトルや時間情報などは、コンテンツ一覧画面の画像情報に変換されてディスプレイに出力されることも可能であり、これによって、ユーザは記録媒体３００にどのようなコンテンツが記録されているかを知ることが可能となる。このとき、上記の電子署名の照合で記録時と再生時で装置又は記録媒体３００が異なっており、コンテンツの復号が不可能となっているコンテンツについては、そのコンテンツは内容を再生できないことを示すマークを付けるなどの方法で、ユーザに知らせることが可能である。

【００７３】また、電子署名の照合で記録時と再生時で装置も記録媒体３００も一致していることが確認されたときでも、コンテンツ一覧画面において、他の装置でも再生可能か否かを示すマークの表示を行うことも可能である。このように、ユーザに対して再生可否の分類を表示することにより、ユーザがそのコンテンツに関する制限を知ることが可能となり、例えば他の情報再生装置でも再生できると思って、実際に他の情報再生装置での再生を試みたが再生がうまく行えなかったというようなトラブルを防止できる。

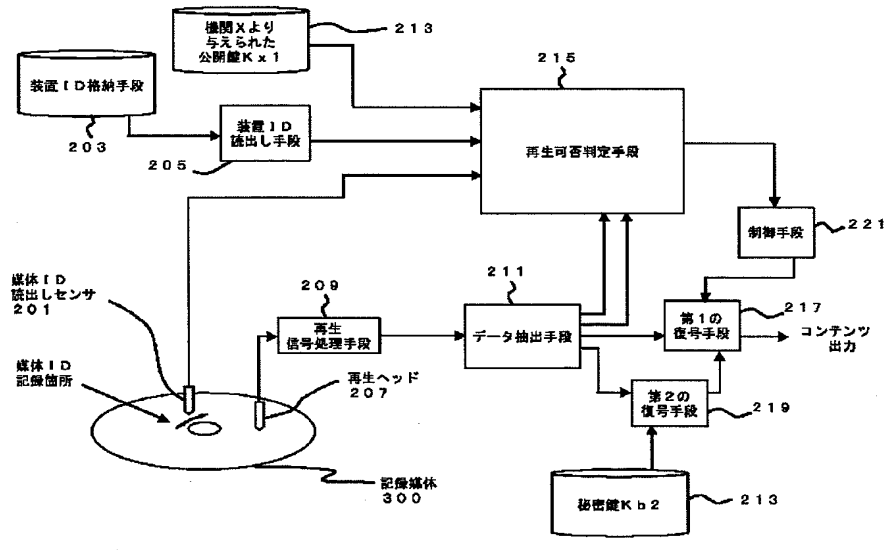
【００７４】また、管理情報を再生する際に、記録媒体３００に複数のコンテンツが存在し、それらが複数の情報記録装置によって記録されたものである場合、情報記録装置毎に記録内容を分類して表示する機能を持たせることも可能である。

【００７５】
【発明の効果】以上説明したように、コンテンツの記録の際に、そのコンテンツを記録する情報記録装置を識別可能とする装置ＩＤ又は情報記録装置が属するグループを識別可能とするグループＩＤと、そのコンテンツを記録する記録媒体を識別可能とする媒体ＩＤとを、コンテンツとともに記録媒体に記録するので、どの情報記録装置又はどのグループに属する情報記録装置によってどの記録媒体にコンテンツが記録されたかという情報を、コンテンツとともに記録媒体に記録することが可能となる。
【００７６】また、コンテンツの再生の際に、コンテンツとともに記録されている装置ＩＤ又はグループＩＤと媒体ＩＤの２つのパラメータを参照して、コンテンツの再生可否の判定を行うので、２重にコンテンツを保護し、コンテンツが不正に複製されることを防ぐことが可能となる。
【００７７】また、コンテンツの記録の際に、そのコンテンツを記録する情報記録再生装置を識別可能とする装置ＩＤと、そのコンテンツを記録する記録媒体を識別可能とする媒体ＩＤとを、コンテンツとともに記録媒体に記録し、コンテンツの再生の際に、記録媒体に記録されている装置ＩＤがこの情報記録再生装置の装置ＩＤと同一であり、かつ情報記録再生装置で記録された記録媒体と同一の記録媒体である場合のみコンテンツの再生を可能とするので、ただ１つの情報記録再生装置でのみ再生が可能となるように、記録媒体にコンテンツを記録することが可能となる。
【００７８】また、情報記録装置にコンテンツを供給する際に、コンテンツとそれに関連する付加情報が供給されて、その付加情報を基にしてコンテンツの記録条件の制御を行うので、例えばコンテンツの供給者又は作成者により、コンテンツの記録再生条件を指定することが可能となり、コンテンツに存在する著作権の保護の度合いをコンテンツの供給者又は作成者が指定することが可能となる。
【００７９】また、コンテンツの記録の際に、そのコンテンツのタイトルや時間情報などを示す管理情報に関しては、従来の再生方法で読出し可能なように記録するので、その記録媒体にどのようなコンテンツがどの時間位置に記録されているか、記録媒体の残り容量はどれくらいかなどのコンテンツの記録に付随して発生する管理情報を、すべての情報再生装置において確認することが可能となる。
【図面の詳細な説明】
【図１】本発明の情報記録装置に係る一実施形態を示す模式図である。
【図２】本発明の情報再生装置に係る一実施形態を示す模式図である。
【図３】本発明の情報記録装置に係る処理動作の一例を示すフローチャートの１枚目である。
【図４】本発明の情報記録装置に係る処理動作の一例を示すフローチャートの２枚目である。
【図５】本発明の情報再生装置に係る処理動作の一例を示すフローチャートの１枚目である。
【図６】本発明の情報再生装置に係る処理動作の一例を示すフローチャートの２枚目である。
【図７】図６に示すフローチャートのステップＳ３６におけるコンテンツの再生可否の判定の動作の一例を示すフローチャートである。
【図８】本発明の情報記録装置に係るコンテンツとともに管理情報を記録する一実施形態を示す模式図である。
【図９】本発明の情報記録装置に係るコンテンツとともに管理情報を記録する処理動作の一例を示すフローチャートである。
【図１０】管理情報TypeI、管理情報TypeII、管理情報TypeIIIの一例を示す図である。
【図１１】本発明の情報再生装置に係るコンテンツ及び管理情報が記録された記録媒体を再生する一実施形態を示す模式図である。
【符号の説明】
１０１、２０１　媒体ＩＤ読出しセンサ
１０３、２０３　装置ＩＤ格納手段
１０５、２０５　装置ＩＤ読出し手段
１０７　結合手段
１０９、２１３　鍵格納手段
１１１　電子署名作成手段
１１３　電子署名付加手段
１１５　暗号化用鍵作成手段
１１７　第１の暗号化手段
１１９　第２の暗号化手段
１２１　フォーマット化手段
１２３　記録信号処理手段
１２５　記録ヘッド
１２７　データ分離手段
１２９　管理情報作成手段
１３１　メモリ
１３３　入力選択手段
２０７　再生ヘッド
２０９　再生信号処理手段
２１１　データ抽出手段
２１５　再生可否判定手段
２１７　第１の復号手段
２１９　第２の復号手段
２２１　制御手段
３００　記録媒体

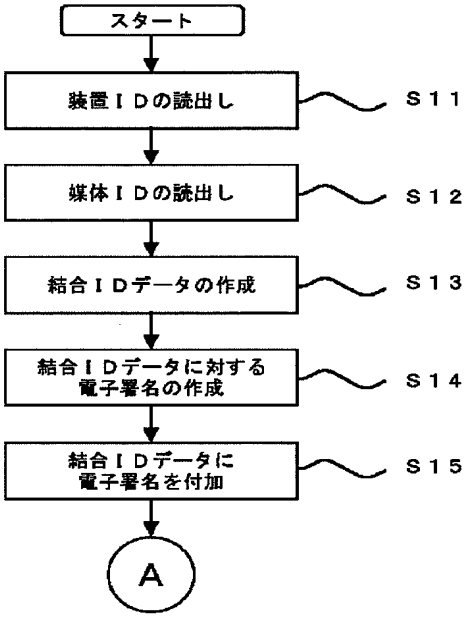
【図１】


秘密鍵Ｋｓ２
109
装置ＩＤ格納手段
103
機関Ｘにより
署名が与えられた
公開鍵Ｋｓ１
109
111
107
電子署名
作成手段
105
装置ＩＤ
読出し手段
結合手段
113
電子署名
付加手段
媒体ＩＤ
読出しセンサ
101
123
121
117
記録
信号処理手段
フォーマット化
手段
第１の
暗号化
手段
コンテンツ
入力
媒体ＩＤ
記録箇所
記録ヘッド
125
119
第２の
暗号化
手段
暗号化用鍵
作成手段
記録媒体
300
109
公開鍵Ｋｂ１
115

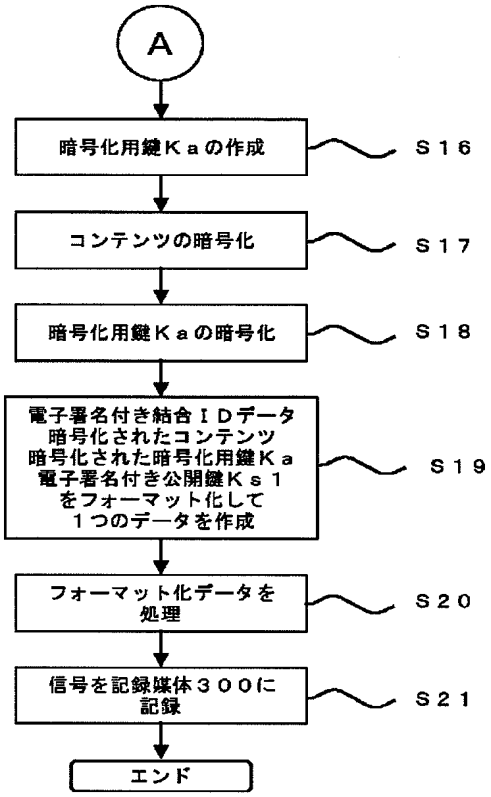
【図２】


機関Ｘより
与えられた
公開鍵Ｋｘ１
213
215
装置ＩＤ格納手段
203
装置ＩＤ
読出し手段
205
再生可否判定手段
制御手段
221
媒体ＩＤ
読出しセンサ
201
209
211
217
再生
信号処理手段
データ抽出手段
第１の
復号手段
コンテンツ
出力
媒体ＩＤ
記録箇所
再生ヘッド
207
第２の
復号手段
219
記録媒体
300
秘密鍵Ｋｂ２
213

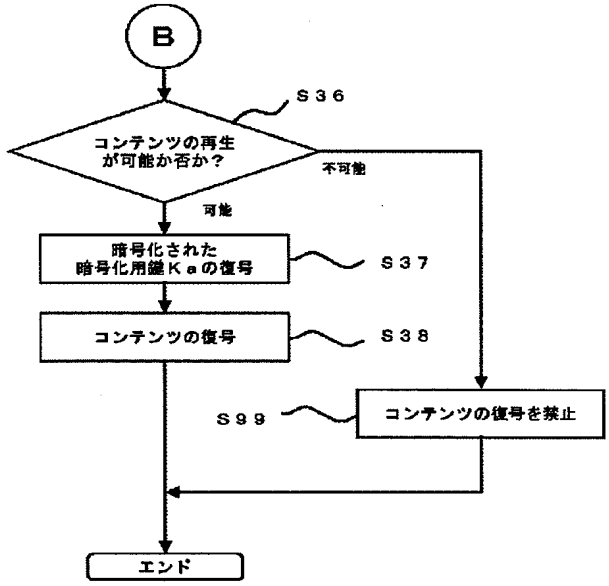
【図３】



【図４】



【図６】



【図１０】

（ａ） TypeⅠ

番組番号
タイトル
信号仕様
記録仕様
再生制約情報（Ｑ＝１１）
電子署名付結合ＩＤ情報
公開鍵Ｋｓ１情報
コンテンツの暗号化の有無
暗号化された暗号化用鍵Ｋａ
記録位置情報
記録時間情報

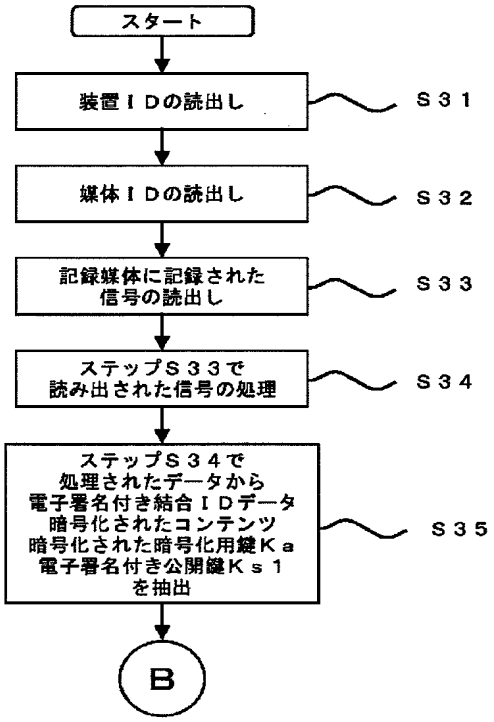
（ｂ） TypeⅡ

番組番号
タイトル
信号仕様
記録仕様
再生制約情報（Ｑ＝１０）
電子署名付結合ＩＤ情報
機器グループ情報
公開鍵Ｋｓ１情報
コンテンツの暗号化の有無
暗号化された暗号化用鍵Ｋａ
記録位置情報
記録時間情報

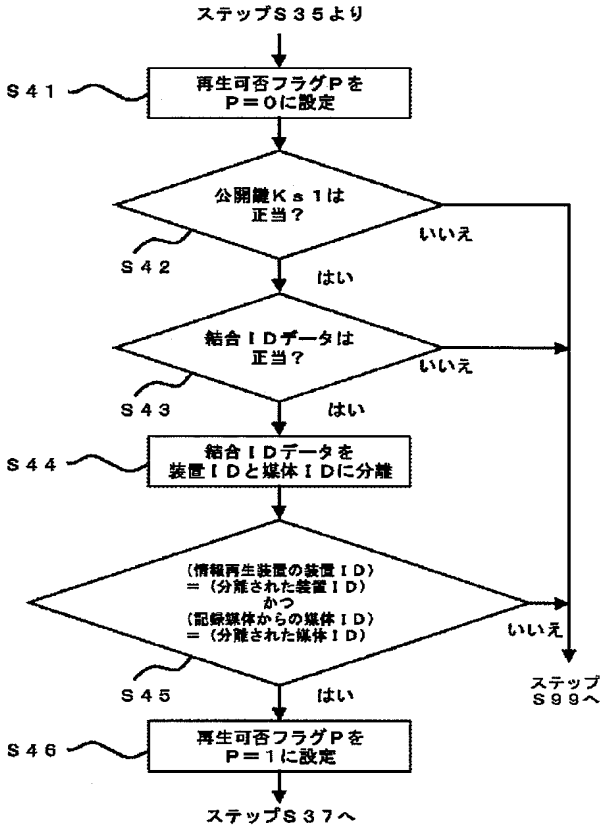
（ｃ） TypeⅢ

番組番号
タイトル
信号仕様
記録仕様
再生制約情報（Ｑ＝００）
コンテンツの暗号化の有無
暗号化された暗号化用鍵Ｋａ
記録位置情報
記録時間情報

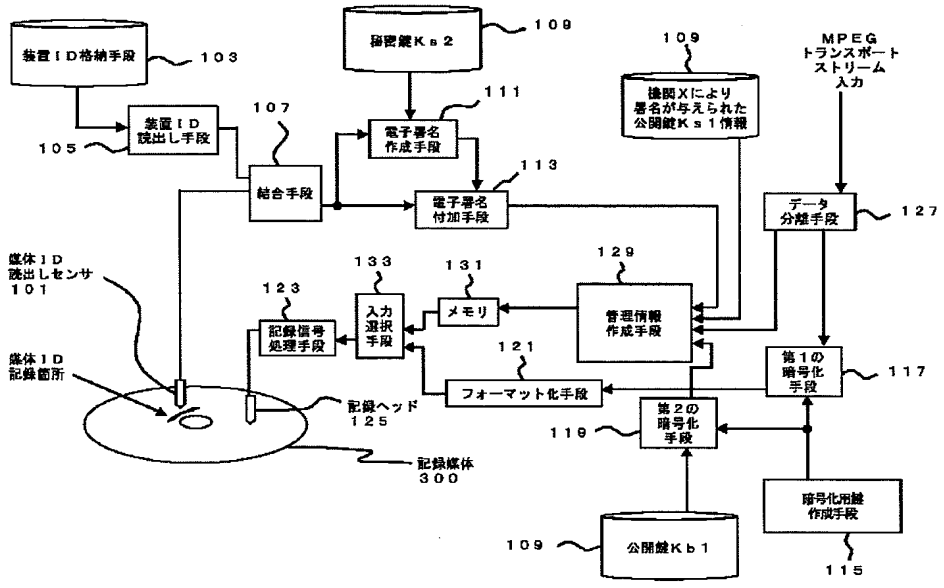
【図５】


スタート
装置ＩＤの読出し
Ｓ３１
媒体ＩＤの読出し
Ｓ３２
記録媒体に記録された信号の読出し
Ｓ３３
ステップＳ３３で読み出された信号の処理
Ｓ３４
ステップＳ３４で処理されたデータから電子署名付き結合ＩＤデータ 暗号化されたコンテンツ 暗号化された暗号化用鍵Ｋａ 電子署名付き公開鍵Ｋｓ１を抽出
Ｓ３５
B

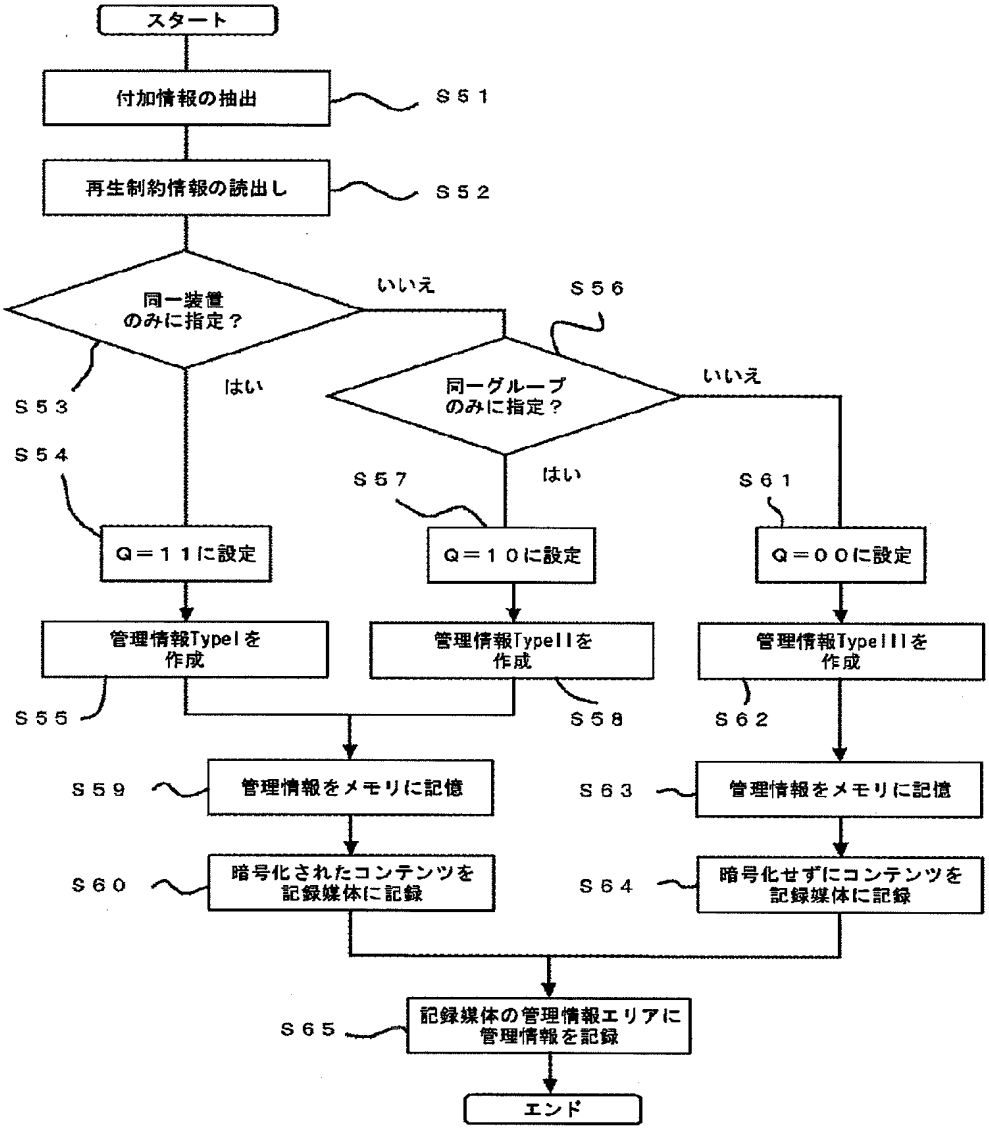
【図７】


ステップＳ３５より
Ｓ４１
再生可否フラグＰをＰ＝０に設定
公開鍵Ｋｓ１は正当？
いいえ
Ｓ４２
はい
結合ＩＤデータは正当？
いいえ
Ｓ４３
はい
Ｓ４４
結合ＩＤデータを装置ＩＤと媒体ＩＤに分離
（情報再生装置の装置ＩＤ）＝（分離された装置ＩＤ）かつ（記録媒体からの媒体ＩＤ）＝（分離された媒体ＩＤ）
いいえ
ステップＳ９９へ
Ｓ４５
はい
Ｓ４６
再生可否フラグＰをＰ＝１に設定
ステップＳ３７へ

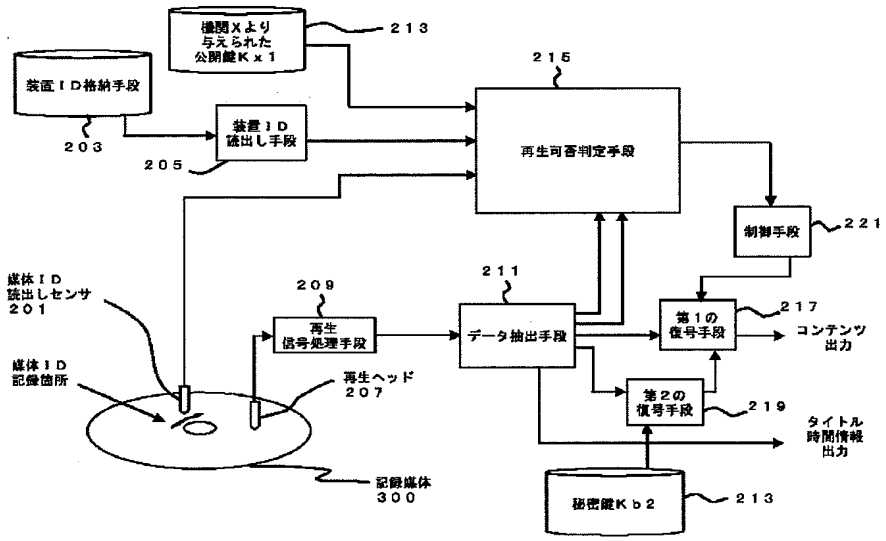
【図８】


装置ＩＤ格納手段
103
秘密鍵Ｋｓ２
109
109
MPEG トランスポートストリーム入力
機関Ｘにより署名が与えられた公開鍵Ｋｓ１情報
105
装置ＩＤ読出し手段
107
111
電子署名作成手段
結合手段
113
電子署名付加手段
データ分離手段
127
媒体ＩＤ読出しセンサ 101
123
133
131
129
記録信号処理手段
入力選択手段
メモリ
管理情報作成手段
媒体ＩＤ記録箇所
121
第１の暗号化手段
117
フォーマット化手段
記録ヘッド 125
第２の暗号化手段
119
記録媒体 300
暗号化用鍵作成手段
109
公開鍵Ｋｂ１
115

【図９】


スタート
付加情報の抽出
Ｓ５１
再生制約情報の読出し
Ｓ５２
同一装置のみに指定？
いいえ
Ｓ５６
Ｓ５３
はい
同一グループのみに指定？
いいえ
Ｓ５４
Ｓ５７
はい
Ｓ６１
Ｑ＝１１に設定
Ｑ＝１０に設定
Ｑ＝００に設定
管理情報TypeIを作成
管理情報TypeIIを作成
管理情報TypeIIIを作成
Ｓ５５
Ｓ５８
Ｓ６２
Ｓ５９
管理情報をメモリに記憶
Ｓ６３
管理情報をメモリに記憶
Ｓ６０
暗号化されたコンテンツを記録媒体に記録
Ｓ６４
暗号化せずにコンテンツを記録媒体に記録
Ｓ６５
記録媒体の管理情報エリアに管理情報を記録
エンド

【図１１】



フロントページの続き

Ｆターム(参考)　5B017 AA06 BA09 BB00 CA00 CA06
CA09
5B065 BA03 BA07 CA11 PA04 PA13
PA14
5C053 FA13 GB06 GB11 JA01 JA21
KA05
5D044 AB05 AB07 BC04 CC06 DE29
DE49 DE50 EF05 FG18 GK12
HL02 HL08
5J104 AA09 AA13 LA03 LA06 NA05
PA14